KUTAKROCK

Kutak Rock LLP
The Omaha Building, 1650 Farnam Street, Omaha, NE 68102-2103
office 402.346.6000

Todd C. Kinney
402.346.6000
todd.kinney@kutakrock.com

February 12, 2021

Office of the Attorney General
Consumer Protection and Antitrust
Gateway Professional Center
1050 E Interstate Avenue Suite 200
Bismarck, ND 58503-5574
Email: ndag@nd.gov

Re: Notice of Data Security Incident

To Whom it May Concern:

Pursuant to N.D.C.C. § 51-30-02, this email is intended to serve as notice to Attorney General's Office concerning a recent privacy issue at Grand River Medical Group, P.C. ("Grand River").

Grand River is a hospital, with its principal place of business located at 1515 Delhi Street, Suite 100 Dubuque, IA 52001. An unauthorized individual gained access into a Grand River employee's email account, which allowed the unauthorized person to potentially view confidential spreadsheets containing individuals' personal information. There were three North Dakota resident affected. The data involved is the following: name, date of birth, visit type, and provider's name. Grand River mailed notices to affected individuals, including three North Dakota residents, starting from February 8, 2021 through February 11, 2021. I have attached a copy of that notice.

Once the incident was discovered, Grand River immediately began investigating and terminated the attacker's access. Grand River examined the affected email account as well as the company's entire network to rule out other suspicious activity. Grand River also commissioned an outside incident response firm, which specializes in these types of incidents, to conduct a forensic analysis to determine whether any data was accessed or exfiltrated (downloaded) by the intruder. Grand River immediately changed all relevant passwords and the compromised account was isolated from the system. Additionally, the company has implemented all of the additional safeguards recommended by its third-party forensic consultants in order to prevent similar attacks in the future. The forensic analysis did not reveal any evidence of data access or exfiltration, however, Grand River still provided notice out of an abundance of caution.

In addition, Grand River is offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: 12 months of

credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy and fully managed id theft recovery services. Grand River has no evidence to suggest that personal information has been misused at this time but has encouraged affected individuals to take full advantage of these identity theft protection services.

Please let us know if you have any additional questions regarding this incident.

Sincerely,

Todd C. Kinney

TCK

Grand River Medical Group, P.C.

C/O IDX
PO Box 4129
Everett WA 98204

ENDORSE
NAME
ADDRESS1
ADDRESS2
CSZ
COUNTRY
BREAK
SEQ
CODE 2D
Ver 3

To Enroll, Please Call:
833-764-1663
Or Visit:
https://response.idx.us/enrollgrmg
Enrollment Code: <<XXXXXXXX>>

February 8, 2021

Notice of Data Breach

Dear <<First Name>> <<Last Name>>,

We are writing to make you aware of a recent privacy issue at Grand River Medical Group, P.C. ("Grand River"). We take patient privacy very seriously and understand that your personal information is important to you.

What Happened

An unauthorized individual recently gained access into an employee's email account, allowing the individual to potentially view documents containing certain personal information. Once the intrusion was discovered, Grand River immediately terminated the unauthorized individual's access to any part of our system. Grand River promptly engaged outside incident response experts to conduct a forensic analysis of the incident to determine whether any data was accessed or exfiltrated (downloaded) by the intruder. The forensic analysis did not reveal any evidence of data access or exfiltration, but we could not definitively rule such activity out, so we are providing you notice out of an abundance of caution. Because we believe some of your personal information was included in the documents, we are notifying you of the incident.

What Information Was Involved

The documents contained the following information:

- First Name
- Last Name
- Provider's Name
- Visit Type
- Date of Birth

Please note that no social security numbers or any financial information was included on the documents that may have been accessed.

What We Are Doing

As soon as Grand River discovered what happened, we immediately terminated access to the account and began investigating. Our IT department analyzed the entire network for any unauthorized activity. In addition, we hired an outside forensic incident response team which specializes in these types of incidents to determine the extent of the breach. We immediately changed all relevant passwords, added multi-factor authentication, and isolated the compromised account from the system. We have implemented all additional safeguards recommended by our third-party forensic consultants in order to prevent similar attacks in the future. While we do not have any evidence to suggest that your personal information was

actually accessed, exported, or used by the attacker, we recognize that the information involved is sensitive and could be used to commit identity theft.

In addition, we are offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: xx months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. Please note that credit monitoring services are not available for minor children because children typically do not have a credit file before 18 years of age. With this protection, IDX will help you resolve issues if your identity is compromised. We have no evidence to suggest that your information has been misused at this time, but we encourage you to take full advantage of these identity theft protection services.

What You Can Do

You can contact IDX and enroll by calling **833-764-1663** or going to **https://response.idx.us/enrollgrmg** and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is May 8, 2021. Please do not discard this letter: you will need to reference the enrollment code at the top of this letter when calling or enrolling online. We have also included additional information in the Recommended Steps below with contact information for the three major credit bureaus and select government agencies.

For More Information

You will find detailed instructions for enrollment on the enclosed Recommended Steps document. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is May 8, 2021. Please do not discard this letter: you will need to reference the enrollment code at the top of this letter when calling or enrolling online. We have also included additional information in the Recommended Steps below with contact information for the three major credit bureaus and select government agencies.

Please call **833-764-1663** or go to **https://response.idx.us/enrollgrmg** for assistance with any additional questions you may have about enrolling in IDX identity protection.

If you have any questions about the underlying incident, please feel free to call **833-764-1663**.

Sincerely,

Justin C. Hafner, MBA
Chief Executive Officer

(Enclosure)

Recommended Steps to help Protect your Information

1. Website and Enrollment. Go to https://response.idx.us/enrollgrmg and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you. Credit monitoring services are not available for minor children because children typically do not have a credit file before 18 years of age.

3. Telephone. Contact IDX at 833-764-1663 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

SEQ
CODE 2D

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.